BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 55 880.9

Anmeldetag: 29. November 2002

Anmelder/Inhaber: Philips Intellectual Property & Standards GmbH, Hamburg/DE

(vormals: Philips Corporate Intellectual Property GmbH)

Bezeichnung: Elektronisches Kommunikationssystem und Verfahren zum Erkennen einer Relais-Attacke auf dasselbe

IPC: G 07 C, E 05 B, B 60 R

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 26. September 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Eberl

A 9161
02/00
EDV-L

ZUSAMMENFASSUNG

Elektronisches Kommunikationssystem und Verfahren zum Erkennen einer Relais-Attacke auf dasselbe

Um ein elektronisches Kommunikationssystem (100), aufweisend

- mindestens eine Basisstation (10) mit mindestens einer insbesondere spulenförmig ausgebildeten Antenneneinheit (16: 16a, 16b), welche Basisstation (10) insbesondere an oder in einem gegen unbefugte Benutzung und/oder gegen unbefugten Zugang zu sichernden Objekt, wie etwa an oder in einem Fortbewegungsmittel oder an oder in einem Zugangssystem, angeordnet ist, sowie
- mindestens eine insbesondere datenträgerförmig ausgebildete Transponderstation (40) mit mindestens einer insbesondere spulenförmig ausgebildeten Antenneneinheit (44: 44a, 44b), welche Transponderstation (40)
  - -- insbesondere von einem befugten Benutzer mitführbar ist und/oder
  - -- zum Austauschen von Datensignalen (22, 24) mit der Basisstation (10) ausgelegt ist,

wobei mittels der Datensignale (22, 24)

- --- die Benutzungs- und/oder Zugangsberechtigung feststellbar und/oder
- --- die Basisstation (10) entsprechend steuerbar ist,

sowie ein Verfahren zum Erkennen und/oder zum Abwehren mindestens eines insbesondere externen Angriffs, vorzugsweise mindestens einer Relais-Attacke, auf mindestens ein derartiges elektronisches Kommunikationssystem (100) so weiterzubilden, dass der Angriff zumindest wesentlich erschwert, wenn möglich sogar vollständig abgewehrt und verhindert wird, wird vorgeschlagen, dass

- in der Basisstation (10) mindestens ein erstes Verzögerungsglied (17) zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit (t_1) innerhalb der Basisstation (10) angeordnet ist und/oder
- in der Transponderstation (40) mindestens ein zweites Verzögerungsglied (47) zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit (t_2) innerhalb der Transponderstation (40)

angeordnet ist.

Fig. 4

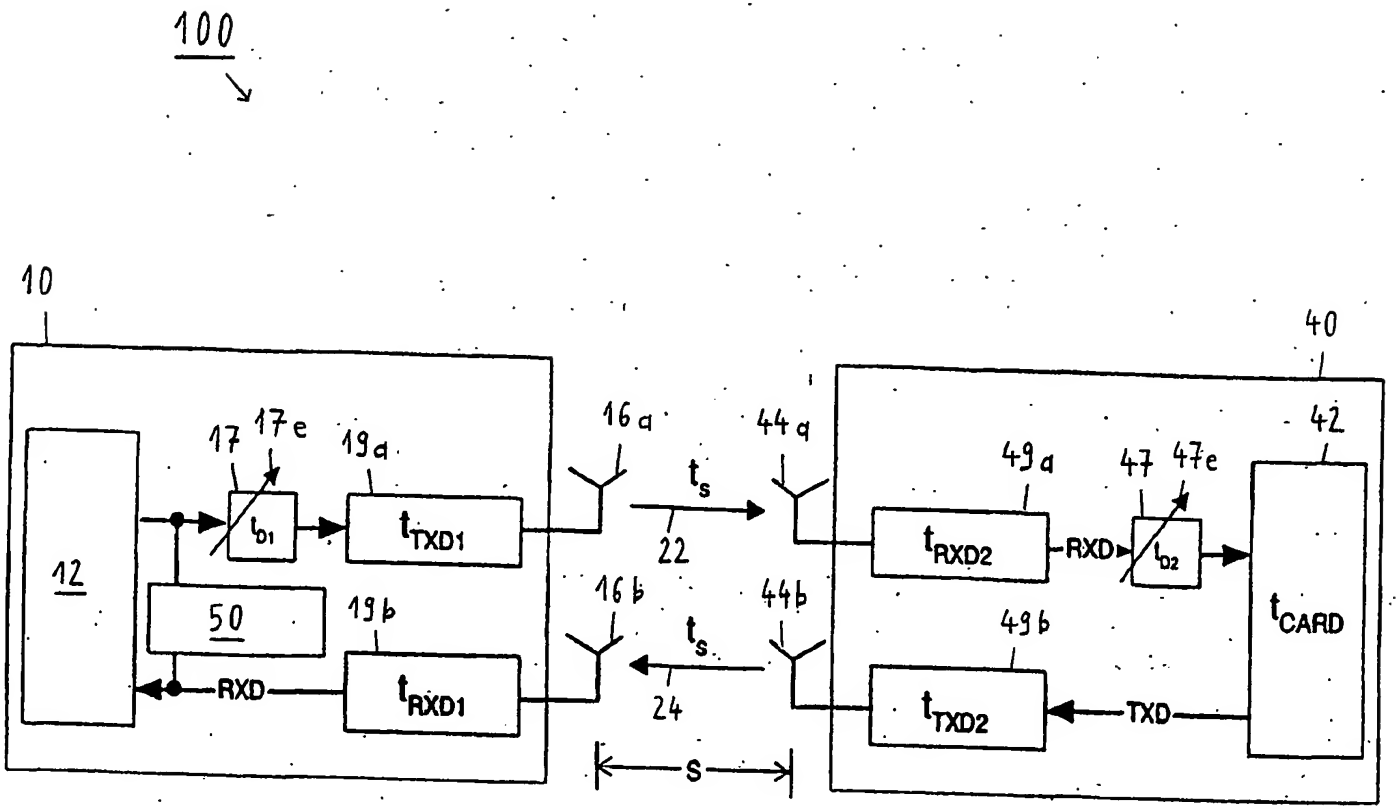
100
10
40
12
50
17
17e
19a
19b
t_{D1}
t_{TXD1}
t_{RXD1}
RXD
16a
16b
t_s
22
24
44a
44b
S
42
49a
49b
47
47e
t_{RXD2}
t_{TXD2}
t_{D2}
t_{CARD}
TXD

Fig. 4

BESCHREIBUNG

Elektronisches Kommunikationssystem und Verfahren zum Erkennen einer Relais-Attacke auf dasselbe

Die vorliegende Erfindung betrifft allgemein das technische Gebiet der Sicherungs- und/oder Zugangssysteme, insbesondere auch der sogenannten P[assive] K[eyless] E[ntry]-Systeme, wie sie beispielsweise im Bereich von Fortbewegungsmitteln und hierbei vor allem im Bereich von Zugangssystemen für Kraftfahrzeuge eingesetzt werden.

Im speziellen betrifft die vorliegende Erfindung ein elektronisches Kommunikationssystem gemäß dem Oberbegriff des Hauptanspruchs sowie ein Verfahren zum Erkennen und/oder zum Abwehren mindestens eines insbesondere externen Angriffs, vorzugsweise mindestens einer Relais-Attacke, auf mindestens ein elektronisches Kommunikationssystem gemäß dem Oberbegriff des Hauptanspruchs.

Zum Realisieren von elektronischen Kommunikationssystemen, insbesondere von P[assive] K[eyless]E[ntry]-Systemen, der eingangs genannten Art, die unter anderem ein herkömmliches passives Transpondersystem aufweisen, sind konventionellerweise verschiedene Konfigurationen im Einsatz. Eine mögliche Konfiguration ist in den Figuren 1A und 1B der Zeichnungen am Beispiel eines P[assive]K[eyless]E[ntry]-Systems für ein Kraftfahrzeug wiedergegeben:

Zwischen einer sogenannten Basisstation 10, die mit einer in Form einer Spule ausgebildeten Antenneneinheit 16 ausgestattet ist, und einer Transponderstation 40 findet eine zum Authentifizieren vorgesehene Kommunikationssequenz in Form von Datenaustausch statt:

Im Detail bestehen zwischen der Basisstation 10 und der Transponderstation 40 als Signalübertragungsverbindungen ein sogenannter "Up-link-frame" 22, der beispielsweise durch mindestens einen L[ow]F[requency]-Kanal mit induktiver Kopplung gebildet ist

und über den Signale von der Basisstation 10 zur Transponderstation 40 übertragen werden, sowie ein sogenannter "Down-link-frame" 24, der beispielsweise durch mindestens einen U[ltra]H[igh]F[requency]-Kanal gebildet ist und über den Signale von der Transponderstation 40 zur Basisstation 10 übertragen werden (alternativ hierzu können sowohl der "Up-link-frame" 22 als auch der "Down-link-frame" 24 jeweils durch mindestens einen L[ow]F[requency]-Kanal gebildet sein; wiederum alternativ hierzu besteht die Möglichkeit, dass sowohl der "Up-link-frame" 22 als auch der "Down-link-frame" 24 jeweils durch mindestens einen U[ltra]H[igh]F[requency]-Kanal gebildet sind).

Nach Betätigen zum Beispiel eines Türgriffs des Kraftfahrzeugs oder eines Tasters an einer Tür des Kraftfahrzeugs beginnt die dem Kraftfahrzeug funktionell und räumlich zugeordnete Basisstation 10 ein als "Challenge" bezeichnetes Signal zu generieren, das über den "Up-link-frame" 22 zur Transponderstation 40 übertragen wird. Daraufhin berechnet eine vorzugsweise mit mindestens einem Mikroprozessor ausgestaltete elektronische Schaltungsanordnung 42 in der Transponderstation 40 mittels eines kryptographischen Algorithmus und mittels eines geheimen Schlüssels aus der "Challenge" eine als "Response" bezeichnete Signalfolge. Dieses "Response"-Signal wird dann von der Transponderstation 40 über den "Down-link-frame" 24 zur Basisstation 10 übertragen.

Die Basisstation 10 vergleicht sodann die "Response" mittels eines gleichen Kryptoalgorithmus und mittels eines gleichen geheimen Schlüssels; bei Identität veranlasst die Basisstation 10 das Öffnen des Türschlosses des Kraftfahrzeugs, das heißt erst wenn die Authentifizierung, zumeist unter Einsatz kryptographischer Methoden, die Transponderstation 40 als gültig erkennt, wird das Türschloss des Kraftfahrzeugs im angegebenen Ausführungsbeispiel geöffnet.

Wird nun diese Schaltungsanordnung ohne weitere technische Zusätze in der in den Figuren 1A und 1B gezeigten Form betrieben, so besteht die Gefahr, dass ein externer Angreifer, der unbefugterweise die Tür des Kraftfahrzeugs zu öffnen versucht, eine nachfolgend beschriebene sogenannte "Relais-Attacke" mit relativ geringem technischem Aufwand durchführen kann.

In den Figuren 2A und 2B ist schematisch eine Anordnung zum Durchführen einer solchen "Relais-Attacke" wiedergegeben. Dazu wird in die Konfiguration gemäß den Figuren 1A und 1B eine "Angreifer-Ausrüstung" in Form einer zusätzlichen Übertragungsstrecke 30 eingebracht, die ein erstes Relais 32 in Form eines Emulators für die Transponderstation, ein zweites Relais 36 in Form eines Emulators für die Basisstation und eine Nachrichtenverbindung 35 zwischen dem ersten Relais 32 und dem zweiten Relais 36 aufweist.

In diesem Zusammenhang ist die Nachrichtenverbindung 35 zwischen dem ersten Relais 32 und dem zweiten Relais 36 als mindestens ein beliebiger bidirektionaler Übertragungskanal ausgestaltbar, der eine beliebige Distanz zwischen dem ersten Relais 32 und dem zweiten Relais 36 erlaubt.

Zum induktiven Ankoppeln an die Antenneneinheit 16 der Basisstation 10 ist das erste Relais 32 in Form des Transponderstationemulators mit einer zugehörigen, in Form einer Spule ausgebildeten Antenneneinheit 34 ausgerüstet; in analoger Weise ist das zweite Relais 36 in Form des Basisstationsemulators zum induktiven Ankoppeln an eine spulenförmig ausgebildete Antenneneinheit 44 der Transponderstation 40 mit einer zugehörigen, in Form einer Spule ausgebildeten Antenneneinheit 38 ausgerüstet.

Ein Angreifer befindet sich nun mit dem ersten Relais 32 unmittelbar am Kraftfahrzeug. Ein zweiter Angreifer begibt sich mit dem zweiten Relais 36 in ausreichende Nähe zur gültigen Transponderstation 40. Ausgelöst zum Beispiel durch Betätigen eines Türgriffs des Kraftfahrzeugs oder eines Tasters an einer Tür des Kraftfahrzeugs sendet die Basisstation 10 des Kraftfahrzeugs ihre "Challenge" mittels des ursprünglichen, das heißt nicht emulierten "Up-link-frame" 22 zum ersten Relais 32.

Von diesem ersten Relais 32 wird die "Challenge" über die vorgenannte Nachrichtenverbindung 35 zum zweiten Relais 36 weitergeleitet. Das zweite Relais 36 emuliert den "Up-link" 22' und gibt so die "Challenge" mittels der spulenförmig ausgebildeten Anten-

neneinheit 38 an die gültige Transponderstation 40 weiter. Nach Berechnen der "Response" in der gültigen Transponderstation 40 antwortet diese Transponderstation 40 dem zweiten Relais 36 durch Übersenden dieser "Response" mittels des ursprünglichen, das heißt nicht emulierten "Down-link-frame" 24.

Von diesem zweiten Relais 36 wird die "Response" über die vorgenannte Nachrichtenverbindung 35 zum ersten Relais 32 weitergeleitet. Das erste Relais 32 emuliert den "Down-link" 24' und gibt so die "Response" mittels der spulenförmig ausgebildeten Antenneneinheit 34 an die gültige Basisstation 10 im Kraftfahrzeug weiter.

Da die "Response" von der authentischen Transponderstation 40 auf Grundlage der authentischen "Challenge" der Basisstation 10 mithilfe des richtigen Kryptoalgorithmus und des richtigen Schlüssels erzeugt wurde, wird die "Response" als gültig anerkannt und die Tür des Kraftfahrzeugs öffnet sich, obwohl der befugte und rechtmäßige Benutzer dies nicht wünscht.

Angesichts der Tatsache, dass heutzutage beispielsweise gerade im Automobilbereich oder im Zutrittsbereich erhöhte Anforderungen an die Funktion und an die Sicherheit bestimmter Komponenten gestellt werden, erscheint die mittels Maßnahmen gemäß den Figuren 2A und 2B sabotierbare Konfiguration gemäß den Figuren 1A und 1B nicht mehr ausreichend sicher.

Dementsprechend sind zum Erkennen und zum Abwehren derartiger "Relais-Attacken" bereits in der Vergangenheit einige Vorschläge gemacht worden; so ist in der Druckschrift EP 1 136 955 A2 beispielsweise eine Anordnung für ein Zugangssicherungssystem (P[assive]K[eyless]E[ntry]-System) offenbart, mittels derer die relative Orientierung der Basisstation 10 und der Transponderstation 40 zueinander berechnet werden kann.

Gemäß einem weiteren Vorschlag wird zum Erkennen und zum Abwehren derartiger "Relais-Attacken" die Zeit zwischen der "Challenge" und der "Response" ermittelt, um

auf diese Weise eine zusätzliche, durch die Verzögerungen der Relaiselektronik und durch die zusätzliche Laufzeit der Signale zwischen den Relaisstationen bedingte zeitliche Verzögerung zu erkennen (Methode der Laufzeitmessung).

Allerdings ist es so gut wie unmöglich, in einem gängigen Transpondersystem mit einer Trägerfrequenz von 125 Kilohertz eine "Relais-Attacke" mittels der Methode der Signallaufzeitmessung erkennen zu können, denn die hohen Genauigkeitsanforderungen an die Zeitmessung können in der Praxis kaum erfüllt werden, wofür Toleranzen der eingesetzten Filter sowie Temperaturprobleme die Hauptgründe sind.

Um also eine "Relais-Attacke" über eine Laufzeitmessung in sicherer und zuverlässiger Weise erkennen zu können, sind an die Genauigkeit der Zeitmessung extrem hohe Ansprüche zu stellen. In Figur 3 ist in schematischer Darstellung das Prinzip einer derartigen Signallaufzeitmessung zum Erkennen der "Relais-Attacke" aus den Fig. 2A und 2B dargestellt, wie es beim in den Fig. 1A und 1B gezeigten Ausführungsbeispiel aus dem Stand der Technik zum Einsatz gelangt. Die Gesamtsignallaufzeit ergibt sich hierbei wie folgt:

$$t_{total} = t_{TXD1} + t_s + t_{RXD2} + t_{CARD} + t_{TXD2} + t_s + t_{RXD1}$$

Kriterium für das Vorliegen einer "Relais-Attacke" ist nun, dass der Abstand s zwischen der Basisstation 10 und der Transponderstation 40, bedingt durch die zusätzliche Relaisstrecke, einen bestimmten, maximal zugelassenen Abstand s_{max} überschreitet. Zum Erkennen eines Relais-Angriffs ist dieser Abstand s, der aus der Laufzeit t_s der Signale 22, 24 und aus der bekannten Ausbreitungsgeschwindigkeit v_s der Signale 22, 24 gemäß der Formel $s = v_s \cdot t_s$ berechnet werden kann, möglichst genau zu ermitteln.

Zu berücksichtigen ist nun jedoch, dass zur gesuchten Signallaufzeit t_s bei einer Signallaufzeitmessung gemäß Figur 3 die zusätzlichen Verzögerungen t_{TXD1}, t_{RXD2}, t_{CARD}, t_{TXD2} und t_{RXD1} hinzukommen. Zum genauen Bestimmen des Abstands s zwischen der Basis-

station 10 und der Transponderstation 40 und damit auch zum Auswählen eines ausreichend geringen, maximal zugelassenen Abstands s_{max} (ohne große Sicherheitsreserve) müssen diese zusätzlichen Signallaufzeitanteile bekannt sein bzw. hinreichend genau bestimmt werden.

Hierbei ist des weiteren zu bedenken, dass in einem praktischen, kostengünstig in großen Stückzahlen zu produzierenden System mit erheblichen, durch die Elektronik der Basisstation 10 und/oder der Transponderstation 40 bedingten Toleranzen $\Box t_{TXD1}$, $\Box t_{TXD2}$, $\Box t_{RXD1}$, $\Box t_{RXD2}$ der Signallaufzeiten zu rechnen ist. Diese Toleranzen ergeben sich aus Alterungseinflüssen, aus Streuungen der eingesetzten Bauelemente und aus Temperatureinflüssen. Falls keine zusätzlichen Maßnahmen ergriffen werden, sind diese Toleranzen zusätzlich beim Bestimmen des Schwellwerts s_{max} zu berücksichtigen.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein elektronisches Kommunikationssystem der eingangs genannten Art sowie ein Verfahren zum Erkennen und/oder zum Abwehren mindestens eines insbesondere externen Angriffs, vorzugsweise mindestens einer Relais-Attacke, auf mindestens ein elektronisches Kommunikationssystem der eingangs genannten Art so weiterzubilden, dass der Angriff zumindest wesentlich erschwert, wenn möglich sogar vollständig abgewehrt und verhindert wird.

Diese Aufgabe wird durch ein elektronisches Kommunikationssystem mit den im Anspruch 1 angegebenen Merkmalen sowie durch ein Verfahren mit den im Anspruch 7 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den jeweiligen Unteransprüchen gekennzeichnet.

Gemäß der Lehre der vorliegenden Erfindung ist

- in der Basisstation mindestens ein erstes einstellbares Verzögerungsglied zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit t_1 innerhalb der Basisstation und/oder
- in der Transponderstation mindestens ein zweites einstellbares Verzögerungsglied zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit t_2 innerhalb der Transponderstation

angeordnet. Erfindungsgemäß wird also eine zusätzliche einstellbare Signalausbreitungsverzögerung in die Übertragungskette eingefügt.

Mittels dieses ersten einstellbaren Verzögerungsglieds bzw. mittels dieses zweiten einstellbaren Verzögerungsglieds kann innerhalb der Basisstation die Signallaufzeit t_1 bzw. innerhalb der Transponderstation die Signallaufzeit t_2 eingestellt werden, so dass der Angriff erkannt wird, wenn die Summe aus der Signallaufzeit t_1 innerhalb der Basisstation, aus der Signallaufzeit t_2 innerhalb der Transponderstation sowie aus der doppelten Signallaufzeit t_s der Datensignale zwischen der Basisstation und der Transponderstation einen definierten Schwellwert $t_{s,max}$ überschreitet.

Die Grundidee der vorliegenden Erfindung besteht also in der Kompensation der Signallaufzeiten von Sende- und Empfangseinheiten von P[assive]K[eyless]E[ntry]-Systemen, wobei durch geeignete technische Maßnahmen (= Anordnen mindestens eines ersten einstellbaren Verzögerungsglieds zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit t_1 innerhalb der Basisstation und/oder Anordnen mindestens eines zweiten einstellbaren Verzögerungsglieds zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit t_2 innerhalb der Transponderstation) eine möglichst konstante Signalausbreitungsverzögerung der Sende- und Empfangsbaugruppen sowohl auf Seiten der Basisstation, zum Beispiel am oder im zu sichernden Kraftfahrzeug, als auch auf Seiten der Transponderstation, zum Beispiel am oder im PKE-Datenträger (PKE-Karte), gewährleistet wird.

Durch geeignetes Regeln und Einstellen der jeweiligen Verzögerung(en) t_{D1} bzw. t_{D2} innerhalb der Basisstation bzw. innerhalb der Transponderstation mittels des jeweiligen zusätzlichen Verzögerungsglieds ergeben sich verbesserte Bedingungen zum Erkennen und/oder zum Abwehren von "Relais-Attacken" gemäß den folgenden Gleichungen:

$t_1 = t_{RXD1} + t_{D1} + t_{TXD1}$ = im wesentlichen konstant;

$t_2 = t_{RXD2} + t_{D2} + t_{CARD} + t_{TXD2}$ = im wesentlichen konstant.

Eine Relais-Attacke liegt nun vor, wenn folgende Schwellwertbedingung erfüllt ist: $t_{s,max} < t_1 + t_2 + 2t_s = t_{RXD1} + t_{D1} + t_{TXD1} + t_{RXD2} + t_{D2} + t_{CARD} + t_{TXD2} + 2t_s$

In einer praktischen Realisierung kann demzufolge vorteilhafterweise ein Vergleich mit einer einmalig definierten festen Schwelle $t_{s,max}$ erfolgen, wobei die Abhängigkeiten der Systemtoleranzen Dt_{TXD1}, Dt_{TXD2}, Dt_{RXD1}, Dt_{RXD2} der Signallaufzeiten in zweckmäßiger Weise berücksichtigt sind.

Gemäß einer besonders erfinderischen Weiterbildung des vorliegenden elektronischen Kommunikationssystems wie auch des Verfahrens zum Erkennen einer Relais-Attacke auf dasselbe kann eine Option zur Temperaturmessung vorgesehen sein, mittels derer eine nachfolgende Kompensation der Temperaturabhängigkeit durch die zusätzlichen Verzögerungsglieder mit dem Ziel bewerkstelligt werden kann, jeweils konstante und insbesondere temperaturunabhängige Gesamtverzögerungen t_1 innerhalb der Basisstation und t_2 innerhalb der Transponderstation zu erzeugen.

Der (Regel-)Algorithmus zum Implementieren des Verfahrens gemäß der vorliegenden Erfindung kann in bevorzugter Weise auch während einer Kommunikation zwischen Basisstation und Transponderstation ausgeführt werden, um einen externen Angriff auf den Regelalgorithmus durch Einmessen der angreifenden Relais zu verhindern. In diesem Fall müssen die Relais die Daten weiterleiten, um nicht das Protokoll zu verletzen.

Gemäß einer zweckmäßigen Ausgestaltungsform der vorliegenden Erfindung kann der Regelalgorithmus zum Erzeugen der Signallaufzeiten t_1 bzw. t_2 nach einer beliebigen Methode ausgeführt sein, wie beispielsweise nach dem Zählverfahren oder nach der Methode der sukzessiven Approximation.

Das vorzugsweise mehrstufige sowie vorzugsweise schaltbare Verzögerungsglied kann in zweckmäßiger Weise beliebige geeignete Elemente bestehen, wie etwa

- mindestens ein mit bekannter Signallaufzeit behaftetes digitales Gatter und/oder
- mindestens ein Filter und/oder
- mindestens ein getaktetes Schieberegister.

Der Fachmann auf dem Gebiet der Kommunikationselektronik, zum Beispiel ein Elektroingenieur mit vertieften Kenntnissen auf dem Gebiet der Sicherheitssysteme, wird besonders zu schätzen wissen, dass durch die vorliegende Erfindung die Realisierung eines gegen externe Angriffe stark resistenten P[assive]K[eyless]E[ntry]-Systems unterstützt wird, das heißt eine starke Erschwerung der sogenannten "Relais-Attacke" mittels genauer Zeitmessung erfolgt. In Korrespondenz hierzu wird eine praxistaugliche Realisierung einer zusätzlichen exakten Zeitmessung zum Detektieren der Relais-Attake bei erhöhter Zuverlässigkeit ermöglicht.

In der praktischen Realisierung der Zeitmessung kann in vorteilhafter Weise bei hoher Genauigkeit ein Vergleich der gemessenen gesamten Signallaufzeit mit einer festen, eng tolerierten Schwelle $t_{s,max}$ erfolgen, wobei kostengünstige Realisierungsmöglichkeiten das elektronische Kommunikationssystem sowie die zugeordnete Methode für den Einsatz in der Massenproduktion sehr interessant machen.

Die vorliegende Erfindung, die sich auch sowohl auf mindestens eine Basisstation gemäß der vorstehend dargelegten Art als auch auf mindestens eine Transponderstation gemäß der vorstehend dargelegten Art erstreckt, kann in vorteilhafter Weise auch in Systemen eingesetzt werden, die in hohem Maße im Bereich sogenannter "Immobilizer"-Systeme (Wegfahrsperren) bei Fortbewegungsmitteln, insbesondere bei Kraftfahrzeugen, Verwendung finden.

Ein weiteres Anwendungsgebiet der vorliegenden Erfindung ist im Bereich der Gebäudesicherung zu sehen, denn das elektronische Kommunikationssystem mit seiner Basisstation wie auch mit seiner Transponderstation eignet sich in vorzüglicher Weise auch zum Realisieren von sicheren Zugangssystemen auf der Basis von Transpondern, insbesondere von Datenträgern, wie etwa von Chipkarten oder von P[assive]K[eyless]E[ntry]-Karten.

Demzufolge kann die Basisstation insbesondere an oder in einem gegen unbefugte Benutzung und/oder gegen unbefugten Zugang zu sichernden Objekt angeordnet sein, wie etwa an oder in einem Fortbewegungsmittel oder an oder in einem Zugangssystem.

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 sowie dem Anspruch 7 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend anhand des durch die Figuren 4 und 5 veranschaulichten Ausführungsbeispiels näher erläutert.

Es zeigt:

Fig. 1A in schematischer Darstellung das auf induktiver Kopplung beruhende Kommunikationsprinzip zwischen einer Basisstation und einer zugeordneten Transponderstation gemäß einem Ausführungsbeispiel aus dem Stand der Technik;

Fig. 1B in schematischer Darstellung das elektrische Ersatzschaltbild des Kommunikationsprinzips aus Fig. 1A;

Fig. 2A in schematischer Darstellung eine sogenannte "Relais-Attacke" auf das in den Fig. 1A und 1B gezeigte Ausführungsbeispiel aus dem Stand der Technik;.

Fig. 2B in schematischer Darstellung das elektrische Ersatzschaltbild der "Relais-Attacke" aus Fig. 2A;

Fig. 3 in schematischer Darstellung das Signallaufzeitmessungsprinzip zum Erkennen der "Relais-Attacke" aus den Fig. 2A und 2B beim in den Fig. 1A und 1B gezeigten Ausführungsbeispiel aus dem Stand der Technik;

Fig. 4 in schematischer Darstellung das auf dem Generieren von konstanten Signallaufzeiten beruhende Messprinzip gemäß der vorliegenden Erfindung zum Erkennen der "Relais-Attacke" aus den Fig. 2A und 2B bei einem Ausführungsbeispiel gemäß der vorliegenden Erfindung; und

Fig. 5 in schematischer Detaildarstellung die Maßnahmen gemäß der vorliegenden Erfindung zum Regeln der zeitlichen Verzögerung der Signalausbreitung innerhalb der Basisstation und/oder innerhalb der Transponderstation auf konstante Signallaufzeitwerte aus Fig. 4.

Gleiche oder ähnliche Ausgestaltungen, Elemente oder Merkmale sind in den Figuren 1A bis 5 mit identischen Bezugszeichen versehen.

Wie Figur 4 anhand eines Ausführungsbeispiels zeigt, wird durch die vorliegende Erfindung ein elektronisches Kommunikationssystem 100 realisiert, das unter anderem ein Transpondersystem (= Transponderstation 40 in Form eines Datenträgers, nämlich einer P[assive]K[eyless]E[ntry]-Karte) aufweist, die wiederum Teil eines Systems zum Öffnen und Verschließen der Türschlösser eines Kraftfahrzeugs ist.

Die PKE-Karte 40 weist eine Empfangseinheit 49a mit Signallaufzeit t_{RXD2} auf, wobei diese Empfangseinheit 49a an eine Antenneneinheit 44a angeschlossen ist und zum Empfangen von Datensignalen 22 von einer Basisstation 10 dient. Des weiteren weist die PKE-Karte 40 eine Sendeeinheit 49b mit Signallaufzeit t_{TXD2} auf, wobei diese Sende-

einheit 49b an eine Antenneneinheit 44b angeschlossen ist und zum Senden von Datensignalen 24 an die Basisstation 10 dient. Der Empfangseinheit 49a nachgeschaltet sowie der Sendeeinheit 49b vorgeschaltet ist eine Steuereinheit 42 (--> Signallaufzeit t_{CARD}) in Form einer Mikrocontrollereinheit, die zum Steuern der PKE-Karte 40 vorgesehen ist.

Eine ebenfalls in Figur 4 dargestellte Basisstation 10 weist eine Empfangseinheit 19b mit Signallaufzeit t_{RXD1} auf, wobei diese Empfangseinheit 19b an eine Antenneneinheit 16b angeschlossen ist und zum Empfangen der Datensignale 24 von einer PKE-Karte 40 dient. Des weiteren weist die Basisstation 10 eine Sendeeinheit 19a mit Signallaufzeit t_{TXD1} auf, wobei diese Sendeeinheit 19a an eine Antenneneinheit 16a angeschlossen ist und zum Senden der vorerwähnten Datensignale 22 an die PKE-Karte 40 dient. Der Empfangseinheit 19b nachgeschaltet sowie der Sendeeinheit 19a vorgeschaltet ist eine Steuereinheit 12 in Form einer Mikrocontrollereinheit, die zum Steuern der Basisstation 10 vorgesehen ist.

Im aktiven Zustand (vgl. Figur 4) der PKE-Karte 40 findet eine zum Authentifizieren bestimmte Kommunikationssequenz in Form von Datenaustausch zwischen der Basisstation 10 und der PKE-Karte 40 statt, wozu Datensignale 22, 24 zwischen der Basisstation 10 und der Transponderstation 40 ausgetauscht werden; mittels dieser Datensignale 22, 24 ist nicht nur die Benutzungs- und/oder Zugangsberechtigung zum Kraftfahrzeug feststellbar, sondern auch die Basisstation 10 entsprechend steuerbar. Im hier beschriebenen P[assive]K[eyless]E[ntry]-Fall kann die Energieversorgung in bevorzugter Weise über mindestens eine Batterieeinheit erfolgen.

Im Detail bestehen zwischen der Basisstation 10 und der PKE-Karte 40 als Signalübertragungsverbindungen ein sogenannter "Up-link-frame" 22, der beispielsweise durch mindestens einen L[ow]F[requency]-Kanal mit induktiver Kopplung gebildet ist und über den Signale von der Basisstation 10 zur PKE-Karte 40 übertragen werden, sowie ein sogenannter "Down-link-frame" 24, der beispielsweise durch mindestens einen U[ltra] H[igh]F[requency]-Kanal gebildet ist und über den Signale von der PKE-Karte 40 zur Basisstation 10 übertragen werden.

Es liegt jedoch auch im Rahmen der vorliegenden Erfindung, wenn beim durch die Figuren 4 und 5 veranschaulichten Ausführungsbeispiel sowohl der "Up-link-frame" 22 als auch der "Down-link-frame" 24 jeweils durch mindestens einen L[ow]F[requency]-Kanal gebildet sind. Wiederum alternativ hierzu besteht beim durch die Figuren 4 und 5 veranschaulichten Ausführungsbeispiel auch die Möglichkeit, dass sowohl der "Up-link-frame" 22 als auch der "Down-link-frame" 24 jeweils durch mindestens einen U[ltra] H[igh]F[requency]-Kanal gebildet sind.

Nach Betätigen zum Beispiel des Türschlosses des Kraftfahrzeugs beginnt die dem Kraftfahrzeug funktionell und räumlich zugeordnete Basisstation 10 ein als "Challenge" bezeichnetes Signal zu generieren, das über den "Up-link-frame" 22 zur PKE-Karte 40 übertragen wird. Daraufhin berechnet eine vorzugsweise mit mindestens einem Mikroprozessor ausgestaltete elektronische Schaltungsanordnung in der PKE-Karte 40 mittels eines kryptographischen Algorithmus und mittels eines geheimen Schlüssels aus der "Challenge" eine als "Response" bezeichnete Signalfolge. Dieses "Response"-Signal wird dann von der PKE-Karte 40 über den "Down-link-frame" 24 zur Basisstation 10 übertragen.

Die Basisstation 10 vergleicht sodann die "Response" mittels eines gleichen Kryptoalgorithmus und mittels eines gleichen geheimen Schlüssels; bei Identität veranlasst die Basisstation 10 das Öffnen des Türschlosses des Kraftfahrzeugs, das heißt erst wenn die Authentifizierung, zumeist unter Einsatz kryptographischer Methoden, die PKE-Karte 40 als gültig erkennt, wird das Türschloss des Kraftfahrzeugs im angegebenen Ausführungsbeispiel geöffnet.

Um nun gegen Relais-Attacken gemäß der anhand der Figuren 2A und 2B beschriebenen Art resistent zu sein, ist in der Basisstation 10 ein erstes Verzögerungsglied 17 angeordnet, das der Steuereinheit 12 nachgeschaltet sowie der Sendeeinheit 19a vorgeschaltet ist und zum Einstellen einer definierten, im wesentlichen konstanten Signallaufzeit t_1 innerhalb der Basisstation 10 dient. In analoger Weise ist in der PKE-Karte 40 ein zweites

Verzögerungsglied 47 angeordnet, das der Empfangseinheit 49a nachgeschaltet sowie der Steuereinheit 42 vorgeschaltet ist und zum Einstellen einer definierten, im wesentlichen konstanten Signallaufzeit t_2 innerhalb der PKE-Karte 40 dient.

Ein externer Relais-Angriff wird nun erkannt, wenn die Summe

- aus der Signallaufzeit t_1 innerhalb der Basisstation 10,
- aus der Signallaufzeit t_2 innerhalb der PKE-Karte 40 sowie
- aus der doppelten (<--> "Hin"-Signal 22 und "Rück"-Signal 24) Signallaufzeit t_s zwischen der Basisstation 10 und der PKE-Karte 40

einen definierten Schwellwert $t_{s,max}$ überschreitet, das heißt wenn die Schwellwertbedingung

$$t_{s,max} < t_1 + t_2 + 2t_s \quad \text{oder}$$

$$t_{s,max} < t_{RXD1} + t_{D1} + t_{TXD1} + t_{RXD2} + t_{D2} + t_{CARD} + t_{TXD2} + 2t_s$$

erfüllt ist, wobei sich

- die Signallaufzeit t_1 innerhalb der Basisstation 10 im wesentlichen
  - aus der Signallaufzeit t_{RXD1} innerhalb der Empfangseinheit 19b,
  - aus der durch das erste Verzögerungsglied 17 bewirkten Signalverzögerungslaufzeit t_{D1} und
  - aus der Signallaufzeit t_{TXD1} innerhalb der Sendeeinheit 19a

  zusammensetzt und sich
- die Signallaufzeit t_2 innerhalb der PKE-Karte 40 im wesentlichen
  - aus der Signallaufzeit t_{RXD2} innerhalb der Empfangseinheit 49a,
  - aus der durch das zweite Verzögerungsglied 47 bewirkten Signalverzögerungslaufzeit t_{D2},
  - aus der Signallaufzeit t_{CARD} innerhalb der Steuereinheit 42 und
  - aus der Signallaufzeit t_{TXD2} innerhalb der Sendeeinheit 49b

  zusammensetzt; t_s ist die einfache Signallaufzeit zwischen der Basisstation 10 und der PKE-Karte 40 und $2t_s$ demzufolge die doppelte Signallaufzeit zwischen der Basisstation 10 und der PKE-Karte 40.

Um nun diese Grundidee der vorliegenden Erfindung, nämlich die Nutzung einer einmalig definierten, konstanten Signalausbreitungsverzögerung t_1 (--> Basisstation 10) bzw. t_2 (--> PKE-Karte 40) der elektronischen Baugruppen zum Senden und Empfangen der zwischen dem Kraftfahrzeug (--> Basisstation 10) und der P[assive] K[eyless] E[ntry]-Karte 40 ausgetauschten Daten, verwirklichen zu können, ist sowohl das erste Verzögerungsglied 17 innerhalb der Basisstation 10 als auch das zweite Verzögerungsglied 47 innerhalb der PKE-Karte 40 einstellbar (vgl. Bezugszeichen 17e bzw. 47e), vierstufig (vgl. Bezugszeichen 17a, 17b, 17y, 17z bzw. 47a, 47b, 47y, 47z) sowie schaltbar (vgl. Bezugszeichen 17s bzw. 47s) ausgebildet, zum Beispiel

- als mindestens ein mit bekannter Signallaufzeit behaftetes digitales Gatter und/oder
- als mindestens ein Filter und/oder
- als mindestens ein getaktetes Schieberegister.

Zum Regeln der Verzögerungszeiten t_1 bzw. t_2 der Signalausbreitung auf einen konstanten Wert bieten sich verschiedene technische Realisierungen an. Im folgenden wird unter Bezugnahme auf die Detaildarstellung der Figur 5 eine einfache und kostengünstige Realisierung unter Verwendung einer Laufzeitregelung zunächst am Beispiel der Basisstation 10 vorgestellt:

Ein von der Basisstation 10 an die PKE-Karte 40 zu übertragender Impuls wird auf das mehrstufige (vgl. Bezugszeichen 17a, 17b, 17y) sowie schaltbare (vgl. Bezugszeichen 17s) erste Verzögerungsglied 17 geleitet. Der verzögerte Impuls wird anschließend dem Transmitter (= Sendeeinheit 19a der Basisstation 10) zugeführt und vom Receiver (= Empfangseinheit 19b der Basisstation 10) direkt, das heißt ohne relevante zusätzliche Verzögerung der Signalausbreitung empfangen. Gleichzeitig wird der Impuls auch durch die gesamte Verzögerungsleitung, das heißt durch alle vier Stufen 17a, 17b, 17y, 17z des ersten Verzögerungsglieds 17 geführt (--> Verzögerungszeit t_1),

Ein der vierten und letzten Stufe 17z des ersten Verzögerungsglieds 17 nachgeschalteter und mit der Empfangseinheit 19b in Verbindung stehender Entscheider (= erste Entscheidereinheit 18 der Basisstation 10) signalisiert der Steuereinheit 12, welcher der beiden Impulse ("verzögerter Impuls" oder "durch die gesamte Verzögerungsleitung geführter Impuls") zuerst an der ersten Entscheidereinheit 18 anliegt.

In Verbindung mit einem in der Steuereinheit 12 implementierten Regelalgorithmus wird das schaltbare Verzögerungsglied 17 so eingestellt bzw. nachgeführt, dass beide Impulse möglichst gleichzeitig eintreffen; in diesem Falle des im wesentlichen gleichzeitigen Eintreffens des verzögerten Impulses und des durch die gesamte Verzögerungsleitung geführten Impulses ist die gewünschte konstante Gesamtverzögerung t_1 der Signalausbreitung generiert.

Im folgenden wird nun unter Bezugnahme ebenfalls auf die Detaildarstellung der Figur 5 die Realisierung unter Verwendung der Laufzeitregelung am Beispiel der PKE-Karte 40 vorgestellt, wodurch veranschaulicht ist, dass das vorgeschilderte Verfahren zum einfachen und kostengünstigen Regeln der Signallaufzeiten in ähnlicher bzw. analoger Weise auch zum Kompensieren der Signallaufzeiten in der PKE-Karte 40 verwendet werden kann:

Ein von der Basisstation 10 an die PKE-Karte 40 übertragener Impuls wird auf das mehrstufige (vgl. Bezugszeichen 47a, 47b, 47y) sowie schaltbare (vgl. Bezugszeichen 47s) zweite Verzögerungsglied 47 geleitet. Gleichzeitig wird der Impuls auch durch die gesamte Verzögerungsleitung, das heißt durch alle vier Stufen 47a, 47b, 47y, 47z des zweiten Verzögerungsglieds 47 geführt (--> Verzögerungszeit t_2).

Ein der vierten und letzten Stufe 47z des zweiten Verzögerungsglieds 47 nachgeschalteter und mit der Sendeeinheit 49b in Verbindung stehender Entscheider (= zweite Entscheidereinheit 48 der PKE-Karte 40) signalisiert der Steuereinheit 42, welcher der beiden Impulse ("verzögerter Impuls" oder "durch die gesamte Verzögerungsleitung geführter Impuls") zuerst an der zweiten Entscheidereinheit 48 anliegt.

In Verbindung mit einem in der Steuereinheit 42 implementierten Regelalgorithmus wird das schaltbare Verzögerungsglied 47 so eingestellt bzw. nachgeführt, dass beide Impulse möglichst gleichzeitig eintreffen; in diesem Falle des im wesentlichen gleichzeitigen Eintreffens des verzögerten Impulses und des durch die gesamte Verzögerungsleitung geführten Impulses ist die gewünschte konstante Gesamtverzögerung t_2 der Signalausbreitung generiert.

Im Ergebnis lässt sich also feststellen, dass durch das elektronische Kommunikationssystem 100 gemäß den Figuren 4 und 5 sowie durch die diesem Kommunikationssystem 100 zugeordnete Methode eine Kompensation der Toleranzen der Signallaufzeiten von Sende- und Empfangseinheiten bewerkstelligt wird, die vorteilhafterweise in P[assive] K[eyless]E[ntry]-Systemen oder in ähnlichen Konfigurationen eingesetzt werden kann. In diesen Systemen ist durch die vorliegende Erfindung eine Form der Laufzeitmessung implementiert, mittels derer ein potentieller externer Angriff über eine sogenannte Relais-Attacke erkannt und/oder abgewehrt werden kann.

Sowohl das vorgestellte elektronische Kommunikationssystem 100 als auch das vorgestellte Verfahren stellen hierbei eine flexible, kosteneffiziente, neue und erfinderische Erweiterung bereits gemäß dem Stand der Technik möglicher Signallaufzeitmessungen dar, damit diese auch unter praktischen Bedingungen eingesetzt werden können. Hierbei werden die Genauigkeit und die Verlässlichkeit des Prinzips zur Zeitmessung (vgl. Zeitmesseinheit 50 in Figur 4) erhöht.

In diesem Zusammenhang werden erfindungsgemäß typische, den Einsatz der Signallaufzeitmessung in der Vergangenheit erschwerende Randbedingungen überwunden, wie etwa

- Streuungen der Signallaufzeiten innerhalb der Sender und Empfänger aufgrund von Toleranzen der Bauelemente;
- Veränderung der Signallaufzeiten innerhalb der Sender und Empfänger aufgrund von Temperatureinflüssen und Alterung; und/oder
- Kostendruck beim Einsatz in der Massenproduktion.

Die vorliegende Erfindung kann mit Vorteil in P[assive]K[eyless]E[ntry]-Systemen eingesetzt werden, die in zunehmendem Maße im Bereich der Zugangssysteme für Kraftfahrzeuge Verwendung finden. Das vorgestellte elektronische Kommunikationssystem 100 sowie das vorgestellte Verfahren eignen sich darüber hinaus auch zum Realisieren von sicheren Zugangssystemen auf der Basis von Chipkarten 40 im Bereich der Gebäudesicherung, wobei die beschriebene Anordnung gemäß den Figuren 4 und 5 in ähnlicher Weise auch zum Abwehren von Relais-Attacken in Zugangs-/Zutrittssystemen angewendet werden kann.

BEZUGSZEICHENLISTE

100	Elektronisches Kommunikationssystem
10	Basisstation
11	erster Widerstand der Basisstation 10
12	Steuereinheit, insbesondere Mikrocontrollereinheit, der Basisstation 10
13	kapazitive Einheit der Basisstation 10
14	Analogschnittstelle der Basisstation 10
15	zweiter Widerstand der Basisstation 10
16	Antenneneinheit der Basisstation 10:
16a	der Sendeeinheit 19a zugeordnete Antenneneinheit der Basisstation 10
16b	der Empfangseinheit 19b zugeordnete Antenneneinheit der Basisstation 10
17	erstes Verzögerungsglied der Basisstation 10:
17a	erste Stufe des ersten Verzögerungsglieds 17
17b	zweite Stufe des ersten Verzögerungsglieds 17
17e	Einstellbarkeit des ersten Verzögerungsglieds 17
17s	Schaltbarkeit des ersten Verzögerungsglieds 17
17y	vorletzte Stufe des ersten Verzögerungsglieds 17
17z	letzte Stufe des ersten Verzögerungsglieds 17
18	erste Entscheidereinheit der Basisstation 10
19a	Sendeeinheit der Basisstation 10
19b	Empfangseinheit der Basisstation 10
22	"Up-link-frame"
22'	"Up-link-frame"-Emulation
24	"Down-link-frame"
24'	"Down-link-frame"-Emulation
30	zusätzliche Übertragungsstrecke
32	erstes Relais in Form eines Emulators für die Transponderstation 40
34	Antenneneinheit des ersten Relais 32
35	Nachrichtenverbindung zwischen erstem Relais 32 und zweitem Relais 36

36 zweites Relais in Form eines Emulators für die Basisstation 10

38 Antenneneinheit des zweiten Relais 36

40 Transponderstation, insbesondere Datenträger, im speziellen P[assive]K[eyless]E[ntry]-Karte

42 Schaltungsanordnung oder Steuereinheit, insbesondere Mikrocontrollereinheit, der Transponderstation 40

44 Antenneneinheit der Transponderstation 40:

44a der Empfangseinheit 49a zugeordnete Antenneneinheit der Transponderstation 40

44b der Sendeeinheit 49b zugeordnete Antenneneinheit der Transponderstation 40

47 zweites Verzögerungsglied der Transponderstation 40:

47a erste Stufe des zweiten Verzögerungsglieds 47

47b zweite Stufe des zweiten Verzögerungsglieds 47

47e Einstellbarkeit des zweiten Verzögerungsglieds 47

47s Schaltbarkeit des zweiten Verzögerungsglieds 47

47y vorletzte Stufe des zweiten Verzögerungsglieds 47

47z letzte Stufe des zweiten Verzögerungsglieds 47

48 zweite Entscheidereinheit der Transponderstation 40

49a Empfangseinheit der Transponderstation 40

49b Sendeeinheit der Transponderstation 40

50 Zeitmessung

s Abstand zwischen der Basisstation 10 und der Transponderstation 40

t_1 Signallaufzeit innerhalb der Basisstation 10

t_2 Signallaufzeit innerhalb der Transponderstation 40

t_{CARD} Signallaufzeit in der Steuereinheit 42 der Transponderstation 40

t_{D1} Verzögerungslaufzeit innerhalb des ersten Verzögerungsglieds 17 der Basisstation 10

t_{D2} Verzögerungslaufzeit innerhalb des zweiten Verzögerungsglieds 47 der Transponderstation 40

t_{RXD1} Signallaufzeit in der Empfangseinheit 19b der Basisstation 10

$\square t_{RXD1}$ Toleranz der Signallaufzeit in der Empfangseinheit 19b der Basisstation 10

t_{RXD2} Signallaufzeit in der Empfangseinheit 49a der Transponderstation 40

$\square t_{RXD2}$ Toleranz der Signallaufzeit in der Empfangseinheit 49a der Transponderstation 40

t_s - Signallaufzeit zwischen der Basisstation 10 und der Transponderstation 40

t_{total} gesamte Signallaufzeit im elektronischen Kommunikationssystem 100

t_{TXD1} Signallaufzeit in der Sendeeinheit 19a der Basisstation 10

$\square t_{TXD1}$ Toleranz der Signallaufzeit in der Sendeeinheit 19a der Basisstation 10

t_{TXD2} Signallaufzeit in der Sendeeinheit 49b der Transponderstation 40

$\square t_{TXD2}$ Toleranz der Signallaufzeit in der Sendeeinheit 49b der Transponderstation 40

v_s Signalausbreitungsgeschwindigkeit zwischen der Basisstation 10 und der Transponderstation 40

PATENTANSPRÜCHE

1. Elektronisches Kommunikationssystem (100), aufweisend

- mindestens eine Basisstation (10) mit mindestens einer insbesondere spulenförmig ausgebildeten Antenneneinheit (16: 16a, 16b), welche Basisstation (10) insbesondere an oder in einem gegen unbefugte Benutzung und/oder gegen unbefugten Zugang zu sichernden Objekt, wie etwa an oder in einem Fortbewegungsmittel oder an oder in einem Zugangssystem, angeordnet ist, sowie
- mindestens eine insbesondere datenträgerförmig ausgebildete Transponderstation (40) mit mindestens einer insbesondere spulenförmig ausgebildeten Antenneneinheit (44: 44a, 44b), welche Transponderstation (40)
  - insbesondere von einem befugten Benutzer mitführbar ist und/oder
  - zum Austauschen von Datensignalen (22, 24) mit der Basisstation (10) ausgelegt ist, wobei mittels der Datensignale (22, 24)
    - die Benutzungs- und/oder Zugangsberechtigung feststellbar und/oder
    - die Basisstation (10) entsprechend steuerbar ist,

dadurch gekennzeichnet,

dass

- in der Basisstation (10) mindestens ein erstes Verzögerungsglied (17) zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit (t_1) innerhalb der Basisstation (10) angeordnet ist und/oder
- in der Transponderstation (40) mindestens ein zweites Verzögerungsglied (47) zum Einstellen einer definierten, insbesondere im wesentlichen konstanten Signallaufzeit (t_2) innerhalb der Transponderstation (40)

angeordnet ist.

2. Kommunikationssystem gemäß Anspruch 1,
dadurch gekennzeichnet,
dass das erste Verzögerungsglied (17) und/oder das zweite Verzögerungsglied (47) einstellbar (e), mehrstufig (a, b, ..., y, z) sowie schaltbar (s) ausgebildet ist und

- mindestens ein mit bekannter Signallaufzeit behaftetes digitales Gatter und/oder
- mindestens ein Filter und/oder
- mindestens ein getaktetes Schieberegister

aufweist.

3. Kommunikationssystem gemäß Anspruch 1 oder 2,
dadurch gekennzeichnet,

- dass der letzten Stufe (17z) des ersten Verzögerungsglieds (17) mindestens eine mit mindestens einer Steuereinheit (12) der Basisstation (10) und/oder mit mindestens einer Empfangseinheit (19b) der Basisstation (10) in Verbindung stehende erste Entscheidereinheit (18) nachgeschaltet ist und/oder
- dass der letzten Stufe (47z) des zweiten Verzögerungsglieds (47) mindestens eine mit mindestens einer Steuereinheit (42) der Transponderstation (40) und/oder mit mindestens einer Empfangseinheit (49a) der Transponderstation (40) in Verbindung stehende zweite Entscheidereinheit (48) nachgeschaltet ist.

4. Basisstation (10) für ein elektronisches Kommunikationssystem (100) gemäß mindestens einem der Ansprüche 1 bis 3,
gekennzeichnet durch

- mindestens eine mit der Basisstation (10) zugeordneten Antenneneinheit (16b) in Verbindung stehende Empfangseinheit (19b) zum Empfangen der Datensignale (24) von der Transponderstation (40),
- mindestens eine mit der Empfangseinheit (19b) in Verbindung stehende, dem ersten Verzögerungsglied (17) vorzugsweise vorgeschaltete Steuereinheit (12), insbesondere Mikrocontrollereinheit, zum Steuern der Basisstation (10),

- das mindestens eine erste Verzögerungsglied (17) zum Einstellen der definierten, insbesondere im wesentlichen konstanten Signallaufzeit (t_1) innerhalb der Basisstation (10) sowie
- mindestens eine dem ersten Verzögerungsglied (17) vorzugsweise nachgeschaltete, mit der Basisstation (10) zugeordneten Antenneneinheit (16a) in Verbindung stehende Sendeeinheit (19a) zum Senden der Datensignale (22) an die Transponderstation (40).

5. Transponderstation (40) für ein elektronisches Kommunikationssystem (100) gemäß mindestens einem der Ansprüche 1 bis 3,
gekennzeichnet durch

- mindestens eine mit der Transponderstation (40) zugeordneten Antenneneinheit (44a) in Verbindung stehende, dem zweiten Verzögerungsglied (47) vorzugsweise vorgeschaltete Empfangseinheit (49a) zum Empfangen der Datensignale (22) von der Basisstation (10),
- das mindestens eine zweite Verzögerungsglied (47) zum Einstellen der definierten, insbesondere im wesentlichen konstanten Signallaufzeit (t_2) innerhalb der Transponderstation (40),
- mindestens eine dem zweiten Verzögerungsglied (47) vorzugsweise nachgeschaltete Steuereinheit (42), insbesondere Mikrocontrollereinheit, zum Steuern der Transponderstation (40) sowie
- mindestens eine der Steuereinheit (42) vorzugsweise nachgeschaltete, mit der Transponderstation (40) zugeordneten Antenneneinheit (44b) in Verbindung stehende Sendeeinheit (49b) zum Senden der Datensignale (24) an die Basisstation (10).

6. Transponderstation gemäß Anspruch 5,
dadurch gekennzeichnet,
dass die Transponderstation (40) in mindestens einem Datenträger, insbesondere in mindestens einer Karte, im speziellen in mindestens einer Chipkarte, angeordnet ist.

7. Verfahren zum Erkennen und/oder zum Abwehren mindestens eines insbesondere externen Angriffs, vorzugsweise mindestens einer Relais-Attacke, auf mindestens ein elektronisches Kommunikationssystem (100) gemäß dem Oberbegriff des Anspruchs 1, dadurch gekennzeichnet,

dass

- innerhalb der Basisstation (10) eine definierte, insbesondere im wesentlichen konstante Signallaufzeit (t_1) und/oder
- innerhalb der Transponderstation (40) eine definierte, insbesondere im wesentlichen konstante Signallaufzeit (t_2)

eingestellt wird, so dass der Angriff erkannt wird, wenn die Summe

- aus der Signallaufzeit (t_1) innerhalb der Basisstation (10),
- aus der Signallaufzeit (t_2) innerhalb der Transponderstation (40) sowie
- aus der doppelten Signallaufzeit (t_s) der Datensignale (22, 24) zwischen der Basisstation (10) und der Transponderstation (40)

einen definierten Schwellwert ($t_{s,max}$) überschreitet.

8. Verfahren gemäß Anspruch 7,
dadurch gekennzeichnet,

[a.1] dass innerhalb der Basisstation (10) ein das an die Transponderstation (40) zu übertragende Datensignal (22) zumindest partiell konstituierender Impuls auf mindestens ein erstes Verzögerungsglied (17) geleitet und

[a.2] anschließend der durch das erste Verzögerungsglied (17) verzögerte Impuls mindestens einer der Basisstation (10) zugeordneten Sendeeinheit (16a) zugeführt sowie von mindestens einer der Basisstation (10) zugeordneten Empfangseinheit (16b) direkt, das heißt ohne relevante zusätzliche Verzögerung empfangen wird,

[b] dass der das an die Transponderstation (40) zu übertragende Datensignal (22) zumindest partiell konstituierende Impuls im wesentlichen gleichzeitig auch durch das gesamte erste Verzögerungsglied (17a, 17b, ..., 17y, 17z) geführt wird,

[c] dass mindestens einer Steuereinheit (12) der Basisstation (10) von mindestens einer der letzten Stufe (17z) des ersten Verzögerungsglieds (17) nachgeschalteten ersten Entscheidereinheit (18) signalisiert wird, ob der verzögerte Impuls (vgl. Verfahrensschritt [a.2]) oder der durch das gesamte erste Verzögerungsglied (17a, 17b, ..., 17y, 17z) geführte Impuls (vgl. Verfahrensschritt [b]) zuerst an der ersten Entscheidereinheit (18) anliegt, und

[d] dass das erste Verzögerungsglied (17) so eingestellt bzw. geschaltet bzw. nachgeführt wird, dass der verzögerte Impuls (vgl. Verfahrensschritt [a.2]) und der durch das gesamte erste Verzögerungsglied (17a, 17b, ..., 17y, 17z) geführte Impuls (vgl. Verfahrensschritt [b]) möglichst gleichzeitig eintreffen.

9. Verfahren gemäß Anspruch 7 oder 8,
dadurch gekennzeichnet,

[e] dass innerhalb der Transponderstation (40) ein das von der Basisstation (10) empfangene Datensignal (22) zumindest partiell konstituierender Impuls auf mindestens ein zweites Verzögerungsglied (47) geleitet wird,

[f] dass der das von der Basisstation (10) empfangene Datensignal (22) zumindest partiell konstituierende Impuls im wesentlichen gleichzeitig auch durch das gesamte zweite Verzögerungsglied (47a, 47b, ..., 47y, 47z) geführt wird,

[g] dass mindestens einer Steuereinheit (42) der Transponderstation (40) von mindestens einer der letzten Stufe (47z) des zweiten Verzögerungsglieds (47) nachgeschalteten zweiten Entscheidereinheit (48) signalisiert wird, ob der verzögerte Impuls (vgl. Verfahrensschritt [e]) oder der durch das gesamte zweite Verzögerungsglied (47a, 47b, ..., 47y, 47z) geführte Impuls (vgl. Verfahrensschritt [f]) zuerst an der zweiten Entscheidereinheit (48) anliegt, und

[h] dass das zweite Verzögerungsglied (47) so eingestellt bzw. geschaltet bzw. nachgeführt wird, dass der verzögerte Impuls (vgl. Verfahrensschritt [e]) und der durch das gesamte zweite Verzögerungsglied (47a, 47b, ..., 47y, 47z) geführte Impuls (vgl. Verfahrensschritt [f]) möglichst gleichzeitig eintreffen.

10. Verwendung mindestens eines elektronischen Kommunikationssystems (100) gemäß mindestens einem der Ansprüche 1 bis 3, insbesondere mindestens einer Transponderstation (40) gemäß Anspruch 5 oder 6, zum Authentifizieren und/oder zum Identifizieren und/oder zum Kontrollieren der Befugnis, ein mittels des Kommunikationssystems (100) zu sicherndes Objekt, wie etwa ein Fortbewegungsmittel oder ein Zugangssystem, zu benutzen, zu betreten oder dergleichen.

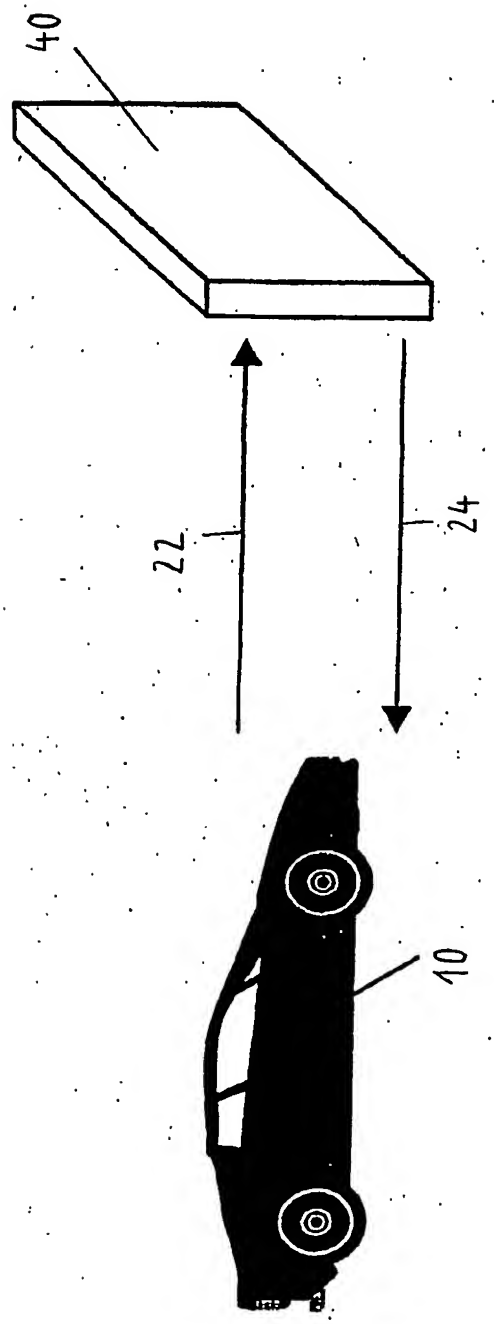

Fig. 1A

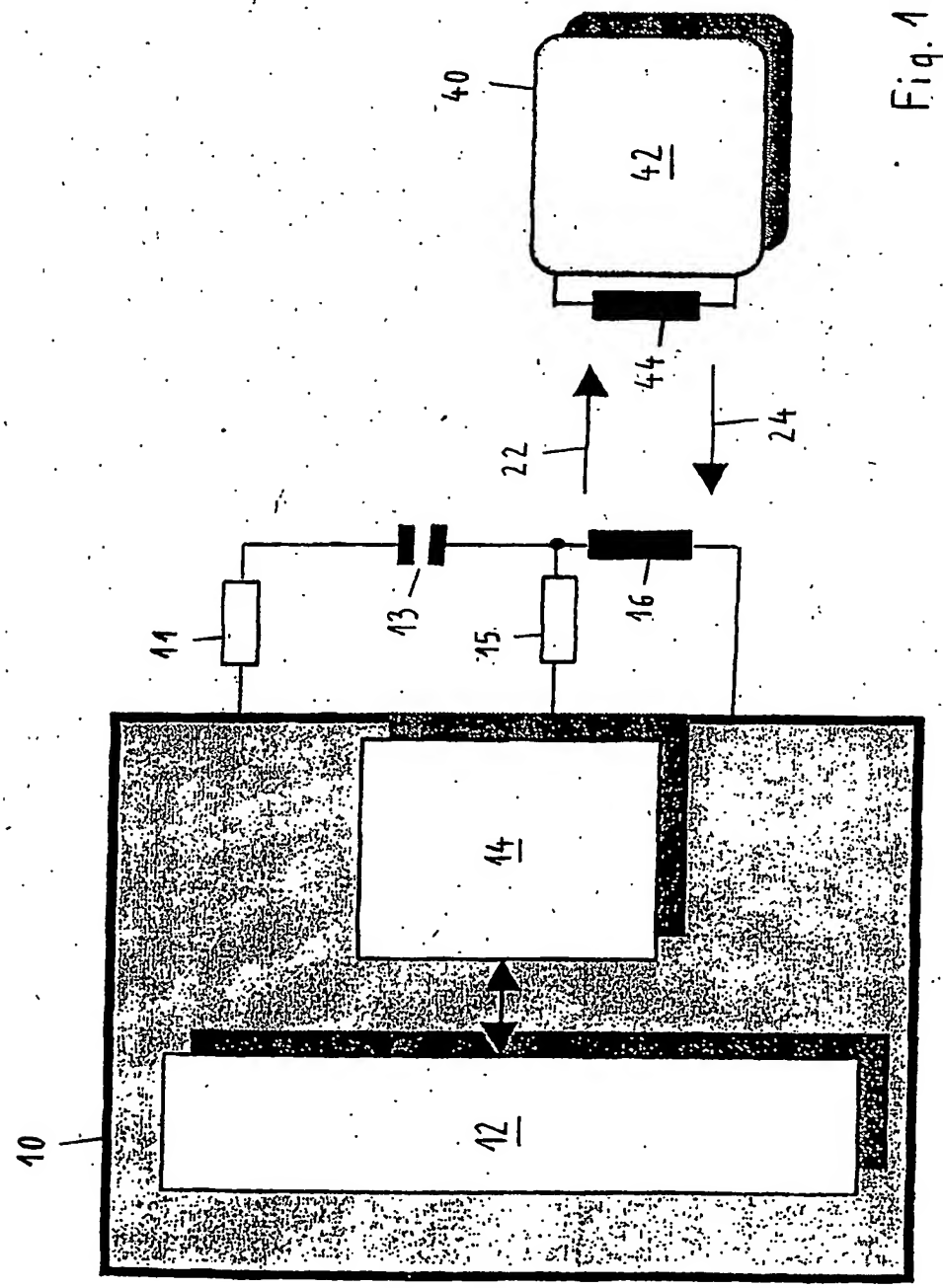

Fig. 1B

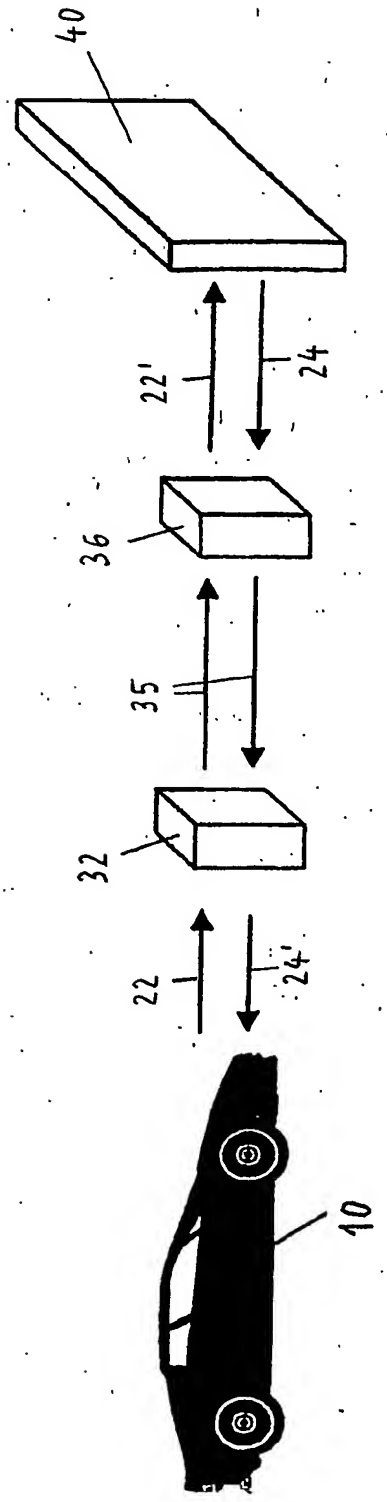

Fig. 2A

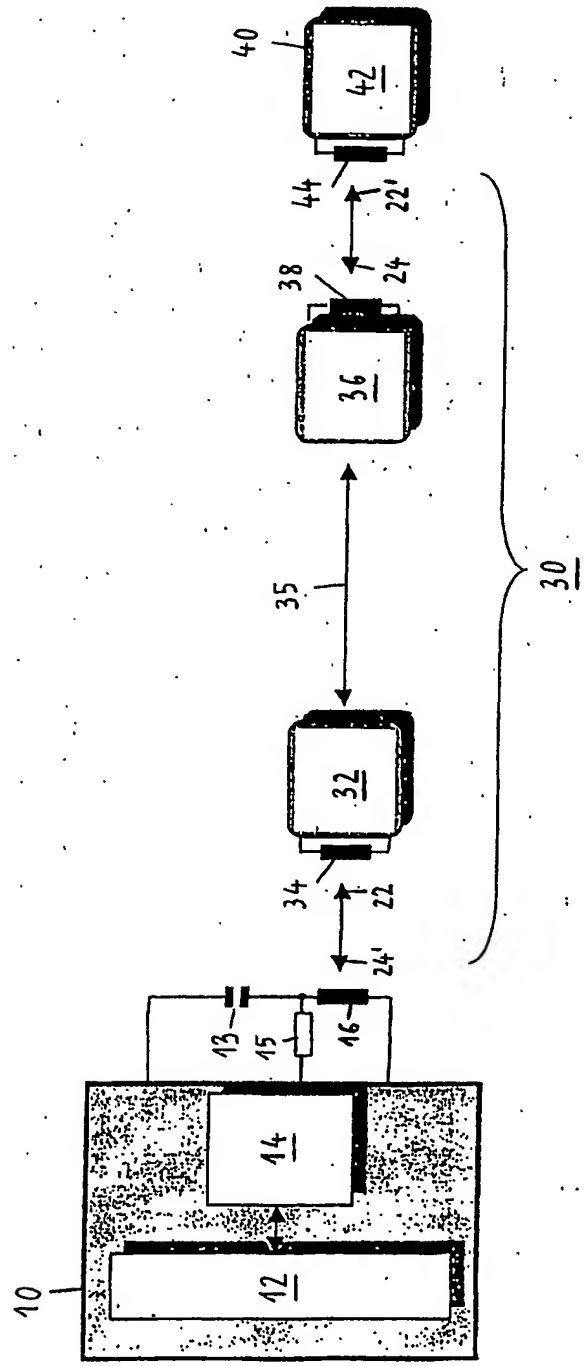

Fig. 2B

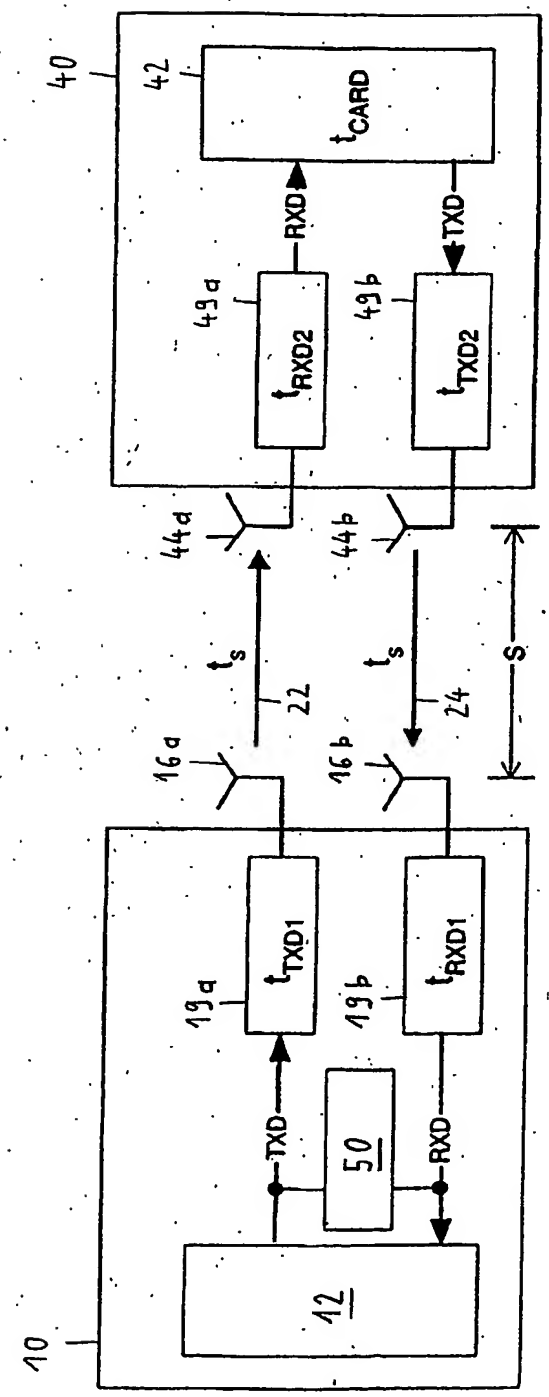
40
42
t_{CARD}
RXD
TXD
49a
49b
t_{RXD2}
t_{TXD2}
44a
44b
t_s
22
t_s
24
S
16a
16b
19a
19b
t_{TXD1}
t_{RXD1}
TXD
50
RXD
12
10

Fig. 3

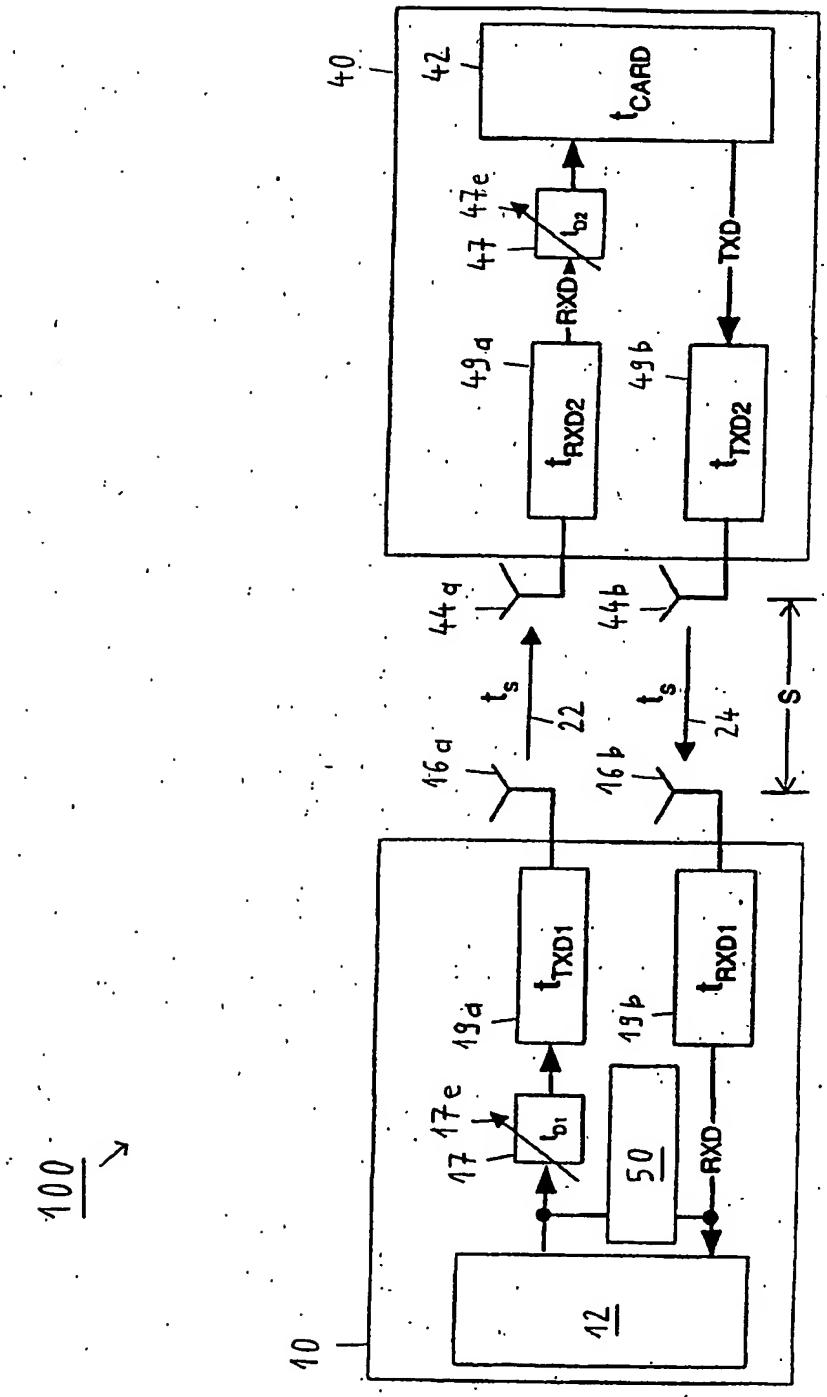
100
10
12
50
17
17e
t_{b1}
19a
t_{TXD1}
19b
t_{RXD1}
RXD
16a
16b
t_s
22
t_s
24
S
44a
44b
40
42
t_{CARD}
47
47e
t_{b2}
RXD
TXD
49a
t_{RXD2}
49b
t_{TXD2}

Fig. 4

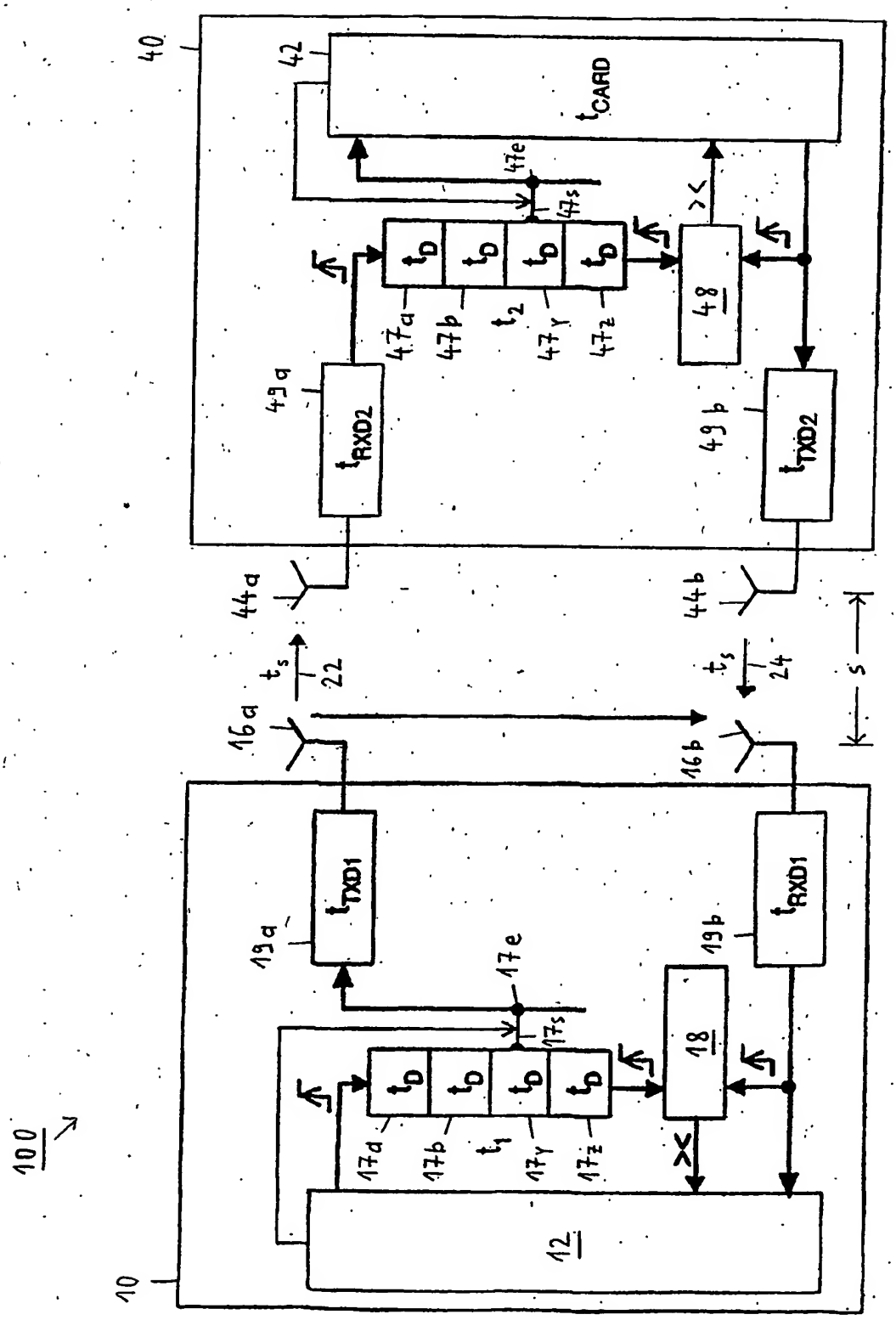
100
10
12
18
48
40
42
t_{CARD}
t_{RXD1}
t_{TXD1}
t_{RXD2}
t_{TXD2}
t_D
t_1
t_2
t_s
s
16a
16b
17a
17b
17e
17s
17γ
17z
19a
19b
22
24
44a
44b
47a
47b
47e
47s
47γ
47z
49a
49b

Fig. 5